Я. В. Кузнецова

Уральский федеральный университет, г. Екатеринбург

Научный руководитель: Г. М. Коркина, к. э. н., доцент

Информационная безопасность интернет-провайдеров региона в условиях инновационного развития бизнеса

Инновационное развитие бизнеса предполагает организованный, систематический процесс поиска и использования нововведений, который немыслим сегодня без информации.

Одним из основных инструментов информационных технологий является глобальная сеть Интернет, предоставляющая возможности инновационных преобразований за счет применения современных средств и методов обмена информацией во всех отраслях экономики, применение Интернет-технологий влечет за собой повышение эффективности бизнеса.

Уральский регион, как и вся страна, насыщен сегодня предприятиями, предоставляющими современные виды связи. Для современного рынка интернет-провайдеров Уральского региона характерен ряд тенденций.

- Большинство ведущих игроков является универсальными операторами связи, предоставляющими комплекс услуг, в том числе телефонию, телевидение и передачу данных. В последние годы наблюдается динамика снижения темпов роста рынка широполосного доступа в Интернет: в 2011 году он вырос на 20 %, в 2012 г.— на 13 %, в 2013 г. — на 10 %.
- Рост цен на услуги интернета не предвидится, он возможен только за счет включения в пакет предложений дополнительных опций.
- В крупных городах УрФО в сфере услуг населению наблюдается насыщенный конкурентами рынок, когда на один жилой микрорайон приходится 6–8 Интернет-провайдеров и до 4–5 компаний, предоставляющих услуги связи. Так, в Екатеринбурге более 13 провайдеров на один дом.

– В связи с тем, что города-миллионники поделены почти полностью, возможность развивать рынок остается лишь при условии охвата сравнительно малых и удаленных населенных пунктов.
– Так как возможности экстенсивного роста во многом исчерпаны, то на первый план стали выходить аспекты повышения качества предоставления услуг.
– Увеличивается скорость передачи данных. Федеральный закон «О связи» 126-ФЗ от 07.07.2003 обязует провайдеров обеспечивать возможность передачи данных со скоростью не менее чем 10 Мбит/с, которая давно им доступна. Крупные игроки рынка стали переходить на более высокие скорости — более чем 100 Мбит/с.
– Расширяются предложения. Наиболее ярким примером является распространение числа пакетных предложений за те же деньги, за которые два—три года назад продавали лишь Интернет. Это позволяет абонентам получать несколько услуг от одного поставщика, а также экономить, поскольку вторая и третья услуги, как правило, предоставляются со скидкой.
– Главными инструментами удержания абонентов являются: бесперебойная работа, оперативная техническая поддержка абонентов, компетентный контактный центр и дополнительные сервисы: игровые площадки, файлообменники, антивирусы и прочий бесплатный и условно бесплатный софт.

Региональный рынок представлен следующими основными компаниями, которые делят между собой около 90 % его объемов.

ОАО «Ростелеком»: работает как первичный магистральный Интернет-провайдер, предоставляющий услуги юридическим лицам, ему принадлежит 38 % регионального рынка.

ОАО «Вымпел-Коммуникации»: акцентирует внимание на развитии сотового направления в качестве ключевого; на него приходится около 11 % рынка.

ОАО «МТС»: обслуживает более 50 тыс. номеров, около половины из которых используется корпоративными абонентами; занимает свыше 10 % рынка региона.

ЗАО «Урал-ТрансТелеКом»: предоставляет широкий спектр телекоммуникационных услуг корпоративным и частным абонентам; ему принадлежит около 20 % регионального рынка.

ЗАО «ЭР-Телеком Холдинг»: Делает ставку на HD-телевидение, высокие скорости и развитие Wi-Fi сети, с долей рынка около 10 %.

Стабильное функционирование интернет-провайдеров во многом зависит от возможностей выявления и устранения внутренних и внешних угроз, которые повышают вероятность неэффективного функционирования компаний, создают неопределенность в достижении ими поставленных целей. Возникающие угрозы, вынуждают операторов связи заниматься обеспечением своей экономической безопасности.

Внешними источниками угроз являются: неблагоприятная экономическая ситуация в мире и в стране, которая вызывает снижение курса национальной валюты, отток капитала, рост уровня инфляции, негативные изменения на отраслевых рынках; действия органов государственной власти когда ими принимаются нормативные документы, которые приводят к ухудшению финансового состояния предприятий; действия других участников отраслевого рынка, способных на проявления недобросовестной конкуренции; необязательность и безответственность контрагентов; форс-мажорные обстоятельства, в том числе природные катаклизмы и военные конфликты, которые нарастают в современном мире.

Внутренние угрозы связаны: с уровнем технической оснащенности производства, своевременным внедрением инноваций и обеспечением технологической независимости предприятия; с квалификацией кадров, степенью их мотивации, уровнем интеллектуального потенциала, с эффективностью менеджмента; с уровнем деловой активности, финансовой независимости и устойчивости работы предприятия; с обеспечением правовой защищенности; с уровнем информационной безопасности работы всех служб и подразделений.

Важным элементом экономической безопасности интернет-провайдера является его информационная защищенность.

Качественное оказание услуг связи предполагает определенный уровень защищенности информационных активов инернет-провайдеров. Информационные активы — это совокупность сведений, средств их обработки и персонала, имеющего к ним.

Политика информационной безопасности любой компании должна включать следующие этапы информационной защищенности: определение перечня информационных и технических ресурсов, подлежащих защите; выявление потенциально возможных внешних и внутренних угроз и каналов утечки информации; оценка рисков и возможного уровня ущерба; определение требований к системе защиты и выбор средств защиты информации; внедрение выбранных способов и средств защиты; управление системой защиты.

Для оценки уровня информационной защищенности специалистами предлагается следующая методика, основанная на выражении экспертного мнения.

Она предполагает сопоставление уровня ущерба, который может быть нанесён предприятию, и средней частоты появления атак, вызывающих данный ущерб, за определённый период времени.

Уровень ущерба оценивается в баллах от 0 до 5 (табл. 1).

Таблица 1

Качественная шкала оценки уровня ущерба

Величина ущерба	Описание
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Фирма прекращает существование

Вероятность атак оценивается экспертом аналогично: в баллах по шкале от 0 до 5 (табл. 2).

Таблица 2

Шкала оценки вероятности атак

Величина ущерба	Описание
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Фирма прекращает существование

Устанавливается перечень возможных атак, которые характерны для рассматриваемого вида деятельности, и по каждому виду атак рассматривается риск.

В соответствии с данной методикой нами проведен расчет рисков системы информационной безопасности ЗАО «Урал-ТрансТелеКом» (Таблица 3)

В качестве максимально допустимого риска задаем значение 10.

Риск на уровне 10 связан с мелкими ошибками в работе сотрудников, которые допускаются практически ежедневно. Так как в компании работает около 350 сотрудников, то данный вид риска становится значимым для ЗАО «Урал-ТрансТелеКом».

Для его уменьшения компании следует систематически повышать уровень квалификации сотрудников и менять систему стимулирования труда, устанавливая дополнительные стимулы за безошибочную работу.

Проверяем каждую строку таблицы на превышение максимального уровня. Таких превышений нет. Однако больше всего приближены к максимальному уровню две внешние атаки: ошибки в информации, предоставляемой контрагентами, и инсинуации от конкурентов. На эти угрозы следует обратить первоочередное внимание при проведении политики экономической безопасности.

Таблица 3

Оценка рисков уровня информационной безопасности ЗАО «УТТК»

Описание атаки	Ущерб	Вероятность	Риск (= Ущерб × × Вероятность)
Внутренние атаки			
Спам (переполнение почтового ящика)	2	2	4
Безопасность рабочего места	3	1	3
Ошибки в работе сотрудников	2	5	10
Технические сбои в программе	1	4	4
Внешние атаки			
Ошибки в информации	2	3	6
Инсинуация	3	2	6
Хищение информации конкурентами	2	2	4
Интегральный риск			37

Инсинуации и хищение информации являются типичными проявлениями недобросовестной конкуренции, и в условиях высококонкурентного рынка интернета, эти угрозы будут нарастать.

Интегральный риск рассматривается как возможность наступления негативных последствий от всех опасностей за заданный интервал времени.

Сравнив интегральный риск 37 с удвоенным значением максимального уровня риска ($10 \times 2 = 20$), получаем, что интегральный риск выше. Это означает, что в системе безопасности набирается множество мелких погрешностей, которые в сумме не дадут предприятию эффективно работать. В этом случае из строк таблицы выбираются те, которые дают самый значительный вклад в значение интегрального риска и производится попытка их уменьшить или устранить полностью.

Так как для ЗАО «Урал-ТрансТелеКом» максимальный риск по атакам достигает 10, то ущерб, причиненный нарушением информационной защищенности, пока является малым и приводит к незначительным потерям для компании. Однако данный риск составляет значительную часть интегрального риска (27 %) и, соответственно, его необходимо устранять.

Таким образом: возможности инновационного развития бизнеса во многом зависят от использования интернет-технологий; региональный рынок интернет-провайдеров связи является высококонкурентным; возможности его экстенсивного роста связаны с расширением географического охвата более отдаленных территорий, однако компании вынуждены всё больше концентрироваться на качественных аспектах: увеличении скоростей, формирования новых пакетных предложений, бесперебойной работе сетей; для экономической безопасности интернет-провайдеров характерны сегодня как внешние угрозы, так и внутренние угрозы; жесткая конкурентная борьба со стороны участников рынка и усиливающаяся в связи с этим недобросовестная конкуренция ведет к необходимости повысить информационную защищенность операторов связи.

Литература

1. *Гончаренко Л. П.* Процесс обеспечения экономической безопасности предприятия // «Справочник экономиста». — 2004. — № 12. — С. 1–3.
2. *Гапоненко В. Ф., Беспалько А. Л., Власков А. С.* Экономическая безопасность предприятий. Подходы и принципы. — М. : Изд-во «Ось-89», 2007. — 208 с.
3. *Губин В. А.* Антикризисная составляющая экономической безопасности хозяйствующего субъекта // «Научные ведомости». 2008. — Вып. 6. — № 2(42). — С. 226–230.
4. «Уралсвязьинформ» купил долю провайдера Кабinet // http://66.ru/news/business/82678
5. ФАС России: Связь под землю загоняют в 36 регионах // http://telekomza.ru/2012/09/04/fas-rossii-svyaz-pod-zemlyu-zagonyayut-v-36-regionax/
6. Подземные кабели влетят в копеечку // http://www.comnews.ru/print?nid=55353
7. «Мотив» готов протянуть коллегам «кабель помощи» // http://urbc.ru/1068015067-alena-yarushina-motiv-gotov-protyanut-kollegam-kabel-pomoschi.html